Attorney Docket No. 1046.1306

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Satoru TANAKA

Application No.: To be Assigned | Group Art Unit: To be Assigned

Filed: January 23, 2004 | Examiner: To be Assigned

For: SECURITY MANAGEMENT DEVICE AND SECURITY MANAGEMENT METHOD

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant submits herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-022630

Filed: January 30, 2003

It is respectfully requested that the applicant be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 23, 2004

By: _____

Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

op1671

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年　１月３０日

出 願 番 号
Application Number: 特願２００３－０２２６３０

[ST. 10/C]: [ＪＰ２００３－０２２６３０]

出 願 人
Applicant(s): 富士通株式会社

２００３年　９月１７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７６５２１

【書類名】　特許願
【整理番号】　0253295
【提出日】　平成15年 1月30日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明の名称】　セキュリティ管理装置及びセキュリティ管理方法
【請求項の数】　10
【発明者】
　【住所又は居所】　東京都稲城市大字大丸１４０５番地　株式会社富士通パソコンシステムズ内
　【氏名】　田中　悟
【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【代理人】
　【識別番号】　100089244
　【弁理士】
　【氏名又は名称】　遠山　勉
【選任した代理人】
　【識別番号】　100090516
　【弁理士】
　【氏名又は名称】　松倉　秀実
　【連絡先】　０３－３６６９－６５７１
【手数料の表示】
　【予納台帳番号】　012092
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティ管理装置及びセキュリティ管理方法

【特許請求の範囲】

【請求項１】

端末のセキュリティレベルを検出するセキュリティ検出部と、

前記端末のセキュリティレベルと所定のレベルとを比較判定する判定部と、

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、当該端末のアクセス許可範囲を制限するアクセス制御部と、

を備えたセキュリティ管理装置。

【請求項２】

前記アクセス制御部は、前記端末のセキュリティレベルが所定のレベルに達していると前記判定部で判定された場合、前記制限範囲より広範囲を当該端末のアクセス許可範囲とする請求項１に記載のセキュリティ管理装置。

【請求項３】

前記アクセス制御部は、前記端末の通信経路を選択する機能を備え、前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合に、当該端末の通信先を特定の装置に変更する請求項１に記載のセキュリティ管理装置。

【請求項４】

前記特定の装置が前記端末のセキュリティレベルを設定する、或は設定の案内を当該端末に提供する請求項３に記載のセキュリティ管理装置。

【請求項５】

コンピュータが、

端末のセキュリティレベルを検出するステップと、

前記端末のセキュリティレベルと所定のレベルとを比較判定するステップと、

前記端末のセキュリティレベルが所定のレベルに達していないと判定された場合、当該端末のアクセス許可範囲を制限するステップと、

を実行するセキュリティ管理方法。

【請求項６】

端末のセキュリティレベルを検出するステップと、

前記端末のセキュリティレベルと所定のレベルとを比較判定するステップと、

前記端末のセキュリティレベルが所定のレベルに達していないと判定された場合、当該端末のアクセス許可範囲を制限するステップと、

をコンピュータにより実行可能なセキュリティ管理プログラム。

【請求項７】

前記端末のセキュリティレベルが所定のレベルに達していると判定された場合、前記制限範囲より広範囲を当該端末のアクセス許可範囲とするステップを含む請求項６に記載のセキュリティ管理プログラム。

【請求項８】

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、前記端末のアクセス許可範囲を制限するステップにおいて、

当該端末の通信経路を選択して通信先を特定の装置に変更する請求項６に記載のセキュリティ管理プログラム。

【請求項９】

前記特定の装置が前記端末のセキュリティレベルを設定する、或は設定の案内を当該端末に提供する請求項８に記載のセキュリティ管理プログラム。

【請求項１０】

セキュリティ管理装置と、ユーザ用の端末と、セキュリティ設定案内装置とをネットワークを介して接続したセキュリティ管理システムとして構成し、

端末のセキュリティレベルを検出するセキュリティレベル検出部と、

前記端末のセキュリティレベルと所定のレベルとを比較判定する判定部と、

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、当該端末のアクセス許可範囲を制限するアクセス制御部と、

を備えたことを特徴とするセキュリティ管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに接続する各端末のセキュリティ状態に応じ、該端末

のアクセスを制限するセキュリティ管理方法及びセキュリティ管理プログラムに関するものである。

【０００２】

【従来の技術】

従来、ＬＡＮ等のネットワークにおいて、セキュリティ性を高める方法として、各端末から不正なアクセスが行なわれないようにゲートウエイ(ファイアウォールを含む)や、ルーター、レイヤ３スイッチのアクセス制限機能により、特定のアドレスを持つ端末の通信を制御する方法が用いられている（特許文献１～６参照）。

【０００３】

【特許文献１】

特開２００２－３３７５６号公報

【特許文献２】

特開２００１－２５６１３６号公報

【特許文献３】

特開平８－３１６９６３号公報

【特許文献４】

特開２０００－１４８２７６号公報

【特許文献５】

特開平６－６３４７号公報

【特許文献６】

特開平１０－１７１８６３号公報

【非特許文献１】

日経産業新聞　２００２年９月２７日　１０頁　先端技術／テクノトレンド　６段目左から８行から～１２行

【０００４】

【発明が解決しようとする課題】

近年、コンピュータは、広く普及し、企業であれば、各社員が専用の端末を有し、これらの端末からそれぞれ電子メールやプリンター等を利用できるようにネ

ットワークを構成することが一般的に行なわれている。

【０００５】

このため、人員の移動や増加に伴って端末も移動や増設するなど、ネットワークに接続する端末を変更する機会が増えてきている。

【０００６】

また、プレゼンテーション等のために携帯端末（ノートパソコン等）を社外に持ち出して利用し、社内ではその携帯端末をネットワークに接続して利用する場合や、携帯端末を自宅に持ち帰って仕事し、その後にこの端末を社内のネットワークに再び接続して仕事の続きを行う場合など、ネットワークに端末を接続する作業が日常的に行なわれている。

【０００７】

このようにユーザが自由に端末の接続を行えると、ウイルス定義ファイルが古いなどセキュリティレベルが低いためにウイルスに感染した端末がネットワークに接続された場合に、該端末が例えば社内ネットワーク外へ不正なアクセスを行ったり、社内ネットワークの他のコンピュータにアクセスしてデータを破壊したりして、ネットワークのセキュリティが脅かされてしまう可能性があった。

【０００８】

しかしながら、ユーザーレベルで端末をネットワークに接続して利用する場合に、その都度ネットワーク管理者が、各端末のセキュリティ状況を確認するのは、セキュリティ管理の手間が懸かり過ぎ、現実的でなかった。

【０００９】

本発明は、このような従来の技術の問題点に鑑みてなされたものである。即ち、本発明の課題は、セキュリティ管理装置が端末のセキュリティレベルに応じて該端末のアクセス制御を行い、セキュリティ設定を促すことにより、セキュリティ管理の省力化を図りつつ所望のセキュリティを確保する技術を提供することにある。

【００１０】

【課題を解決するための手段】

本発明は前記課題を解決するために、以下の手段を採用した。

本発明のセキュリティ管理装置、セキュリティ管理方法、セキュリティ管理プログラム、セキュリティ管理システムは、端末のセキュリティレベルを検出し、前記端末のセキュリティレベルと所定のレベルとを比較判定して、前記端末のセキュリティレベルが所定のレベルに達していないと判定された場合、当該端末のアクセス許可範囲を制限する。

【００１１】

これにより本発明は、端末のセキュリティレベルに応じて該端末のアクセス制御を行い、該端末をセキュリティ設定案内サーバ等の特定の装置にアクセスさせてセキュリティ設定を促すことを可能とし、セキュリティ管理の省力化を図りつつ所望のセキュリティを確保できるようにしている。

【００１２】

〈コンピュータが読み取り可能な記録媒体〉

本発明は、上記のプログラムをコンピュータが読み取り可能に記録した記録媒体であっても良い。そして、コンピュータに、この記録媒体のプログラムを読み込ませて実行させることにより、その機能を提供させることができる。

【００１３】

ここで、コンピュータ読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的、または化学的作用によって蓄積し、コンピュータから読み取ることができる記録媒体をいう。このような記録媒体の内コンピュータから取り外し可能なものとしては、例えばフレキシブルディスク、光磁気ディスク、CD-ROM、CD-R/W、DVD、DAT、８mmテープ、メモリカード等がある。

【００１４】

また、コンピュータに固定された記録媒体としてハードディスクやＲＯＭ（リードオンリーメモリ）等がある。

【００１５】

【発明の実施の形態】

《実施形態１》

以下、本発明の実施形態１に係るセキュリティ管理装置を図１から図５の図面

に基づいて説明する。

【００１６】

〈概略構成〉

図１は本実施形態のセキュリティ管理装置を備えたネットワーク構成例を示す図である。

【００１７】

本実施形態のセキュリティ管理装置１は、複数の端末２が接続され、各端末から送信されたデータのルーティングを行う所謂ルーターである。例えばセキュリティ管理装置１は、該端末２からインターネット上のサーバへのアクセス要求を受け付けた場合、ファイアウォール３を介してインターネット４上のサーバ（不図示）へアクセス要求を送信する。そして該サーバからの応答を受信した場合、セキュリティ管理装置１は、この応答を前記端末に転送する。なお、本実施形態では、このセキュリティ管理装置１をドメイン単位で複数備えている。

【００１８】

このセキュリティ管理装置１は、後に詳述するセキュリティ検出部や、判定部、アクセス制御部として専用に設計された電子回路（ハードウェア）から構成された専用の電子機器であっても良いし、ＣＰＵやメモリ等からなる演算処理部で、本発明のセキュリティ管理プログラムを実行して上記各部の機能をソフトウェア的に実現する装置であっても良い。

【００１９】

また、本実施形態のネットワークには、コンピュータウイルスを特定するためのウイルス定義ファイルを有したウイルス情報サーバ５と、端末が所定のセキュリティレベルに達するように案内するセキュリティ設定案内サーバ６を備えている。

【００２０】

セキュリティ管理装置１は、端末２のセキュリティ情報を検出し、この端末２のセキュリティレベルが所定のレベルに達しているか否かを判定し、このレベルに達していない端末からアクセス要求があった場合、当該端末２をセキュリティ設定案内サーバ６に接続させる。

【００２１】

これに応じ、セキュリティ設定案内サーバ６は、前記端末２が所定のセキュリティレベルを満たすように案内する。例えば、端末２のウイルス定義ファイルが古くてセキュリティレベルが低いと判定された場合、セキュリティ設定案内サーバ６は、該端末２にウイルス情報サーバ５にアクセスして最新のウイルス定義ファイルを取得するように案内する。

【００２２】

このように、本実施形態では、セキュリティレベルが低いと判定された端末２のアクセス許可範囲をセキュリティ設定案内サーバ６とウイルス情報サーバ５に制限し、所定のセキュリティレベルを満たすまで他のコンピュータへのアクセスを許可しないので、万一セキュリティレベルの低い端末２がウイルスに感染しても被害の拡大を防止できる。また、本実施形態では、セキュリティレベルの低い端末２にセキュリティレベルの向上を促し、該端末が他のコンピュータにアクセスする場合には必ず所定のレベルに達していることになるので、ネットワーク管理者が逐一セキュリティレベルを確認しなくても所望のセキュリティが確保できる。

【００２３】

〈セキュリティ管理装置〉

図２は、セキュリティ管理装置１の構成を示すブロック図である。

【００２４】

同図に示すように、セキュリティ管理装置１は、セキュリティ検出部１１や、判定部１２、アクセス制御部１３を備えている。

【００２５】

前記セキュリティ検出部１１は、アクセスパターンによって端末２のセキュリティレベルを検出する。例えばウイルス定義ファイルを備えたサーバ５に前記端末２が所定間隔でアクセスしたか否かをアクセスパターンとして検出する。該セキュリティ検出部１１は、記憶部（メモリ）を備え、前記検出結果を記憶させている。

【００２６】

前記判定部１２は、前記メモリを参照し、セキュリティ検出部１１が検出したセキュリティレベルが所定のレベルに達しているか否かを判定する。

【００２７】

前記アクセス制御部１３は、前記端末２の通信経路を選択する機能を備え、前記端末２のセキュリティレベルが所定のレベルに達していないと判定部１２で判定された場合に、当該端末２のアクセス許可範囲を変更する。例えば、当該端末２のアクセス先を特定のサーバに変更する。

【００２８】

〈セキュリティ管理手順〉

前記セキュリティ管理装置によるセキュリティ管理手順（セキュリティ管理方法）を次に説明する。

【００２９】

図３は、このセキュリティ管理手順を示す説明図である。

セキュリティ管理装置１は、起動すると、先ずセキュリティ検出部１１のメモリ内の検出結果を全て削除（初期化）する（ステップ１、以下Ｓ１のように略記する）。

【００３０】

次にセキュリティ管理装置１のセキュリティ検出部１１は、接続されている端末２のセキュリティレベル、即ち所定の間隔でウイルス情報サーバ５にアクセスしたか否かを検出し、メモリに記憶する（Ｓ２）。この検出は、各端末２に記憶されたログ（何時何処にアクセスしたかの記録）やウイルス定義ファイルの更新時間を読み出すようにしても良いし、ウイルス情報サーバ５に記憶されたログ（どの端末が何時アクセスしたかの記録）を読み出すようにしても良い。

【００３１】

端末２からのアクセスがあった場合、判定部１２は、前記メモリを参照し、この端末２が所定のセキュリティレベルに達しているか否か、即ちアクセス許可の対象であるか否かを判定する（Ｓ３，Ｓ４）。

【００３２】

該端末２がアクセス許可対象と判定された場合、アクセス制御部３は、この端

末２のアクセス許可範囲を全てのコンピュータとし、どのコンピュータに対するアクセスであってもルーティングを行う（Ｓ５）。

【００３３】

一方、ステップ４でアクセス許可対象でないと判定した場合、アクセス制御部１３は、当該端末２のアクセス許可範囲をセキュリティ設定案内サーバ６とウイルス情報サーバ５に制限し、端末２を先ず該サーバ６にアクセスさせる（Ｓ６）。セキュリティ設定案内サーバ６は、接続された端末２にセキュリティに関する設定を案内する画面（ＨＴＭＬによるウエブページ等）を表示させる。図４は、この設定を案内する画面の表示例である。該画面に従って、ユーザは、使用している端末２に必要なウイルス定義ファイルのボタン９９を選択する。該ボタン９９が選択されると、端末２は、このボタン９９のリンク先であるウイルス情報サーバ５に接続し、選択したウイルス定義ファイルを取得する。これにより端末２はアンチウイルスソフトを実行する際に、この最新のウイルス定義ファイルを参照してウイルスを特定し、駆除等を行うことができ、最近発生したウイルスにも対応できる。即ち、セキュリティレベルが向上する。

【００３４】

この端末２がウイルス情報サーバ５にアクセスしたことを検出した場合、セキュリティ検出部１１は、当該端末２を許可対象として前記メモリに追加する（Ｓ７）。

【００３５】

その後、ステップ３に戻ってアクセスがあるまで待機する。

【００３６】

この待機中にネットワークから切断された端末２があった場合、セキュリティ検出部１１は、この端末２の情報を前記メモリから削除する（Ｓ８，Ｓ１０）。また、セキュリティ検出部１１は、メモリに記憶されてから所定時間（本例では２４時間）以上経過した情報を前記メモリから削除する（Ｓ９，Ｓ１０）。

【００３７】

以上のように本実施形態によれば、端末２のセキュリティレベルが所定のレベルに達していない場合、当該端末２のアクセス許可範囲を変更してセキュリティ

設定案内サーバ６及びウイルス情報サーバ５にアクセスさせ、セキュリティレベルの向上を促すことができるので、ネットワークに接続した端末２のセキュリティレベルをネットワーク管理者が逐一確認しなくても所望のセキュリティが確保されることになる。

【００３８】

なお、セキュリティレベルの判定は、上記ウイルス情報サーバへのアクセス間隔に限らず、不要なポートが閉じられているか否か、ＪＡＶＡ（登録商標）やＡｃｔｉｖｅＸ（登録商標）等のプログラムやスクリプトをダウンロードして実行可能であるか否か、Ｐｉｎｇ等の特定のコマンドに応答するか否か、等で判断しても良い。

【００３９】

設定案内サーバ６は、ウイルス情報サーバ５への案内に限らず、セキュリティの設定を行っても良いし、セキュリティ設定用のアプレットを端末２に送信し、このアプレットを端末２に実行させることでセキュリティの設定を行っても良い。なお、このセキュリティの設定とは、ウイルス定義ファイルやアンチウイルスソフトの更新の他、所定のポートを閉じるか否かや、所定のプログラムやスクリプトをダウンロードして実行するか否か、Ｐｉｎｇ等の特定のコマンドに応答するか否か等についての設定である。

【００４０】

また、セキュリティレベルの検出は、端末２上で監査用のプログラムを実行し、検出結果を記憶部に記憶するものでも良い。この検出結果を記憶する記憶部は、セキュリティ管理装置１内であっても良いし、端末２やセキュリティ設定案内サーバ６、ウイルス情報サーバ５等、セキュリティ管理装置１からアクセス可能な装置内にあっても良い。

【００４１】

《変形例１》

図５は前記セキュリティ管理装置を汎用のコンピュータで実現した例を示している。

【００４２】

同図に示すように、セキュリティ管理装置１０は、本体２１内にＣＰＵ（centralprocessing unit）やメインメモリ等よりなる演算処理部２２、演算処理の為のデータやソフトウェア（セキュリティ管理装置等）を記憶した記憶装置２３、入出力部２４、通信制御装置（ＣＣＵ：CommunicationControl Unit）２５等を備えた一般的なコンピュータである。

【００４３】

セキュリティ管理装置１０は、記憶装置２３に記憶されたセキュリティ管理プログラムを読み出して実行することにより、セキュリティ検出部１１や、判定部１２、アクセス制御部１３の機能を実現させている。このときセキュリティ管理装置１０は、前述の実施形態と同様に図３に示した各ステップを実行する。

【００４４】

これにより本例のセキュリティ管理装置１０は、前述の実施形態と同様にネットワーク管理者によるセキュリティ管理の省力化を図りつつ所望のセキュリティを確保することができるようにしている。

【００４５】

《実施形態２》

図６は、本発明の実施形態２の構成を示すブロック図、図７は、本実施形態のセキュリティ管理装置を含めたネットワークの構成図である。本実施形態のメールサーバ（セキュリティ管理装置）２０は、前述の変形例１と比べてメールサーバの機能を備えた点が異なっており、その他の構成は略同じである。なお、同一の要素には同符号を付すなどして再度の説明を省略している。

【００４６】

メールサーバ２０は、メール受信部１４の機能により、インターネット４を介して各端末２宛の電子メールを受信し、接続された端末２に該電子メールを提供する。

【００４７】

また、メールサーバ２０は、メール送信部１５の機能により各端末２から送信メールを受信し、各宛先のコンピュータに送信する。

【００４８】

本実施形態のメールサーバ２０は、端末２がウイルス情報サーバ５にアクセスしてから所定時間以内であれば、メールの送信或は受信を行い、該所定時間を超えていれば、端末２をセキュリティ設定案内サーバ６に接続させる。

【００４９】

これにより本例のメールサーバ２０は、前述の実施形態と同様にネットワーク管理者によるセキュリティ管理の省力化を図りつつ所望のセキュリティを確保でき、セキュリティレベルの低い端末２が接続されたとしても新しいウイルス定義ファイルを取得しなければメールの送受信が行えないため、メールを介したウイルスの被害を招くことが無い。

【００５０】

本実施形態では、メールサーバの例を示したが、本発明のセキュリティ管理装置はこれに限らず、セキュリティ検出部や、判定部、アクセス制御部を備えていれば、プロキシサーバ、ＮＦＳ、ホームゲートウェイ等であっても良い。

【００５１】

《その他の実施形態》

本発明は、上述の図示例にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【００５２】

例えば、上記セキュリティ管理装置１０の実施形態として、アクセス許可範囲の初期設定を全ての範囲にしておき、端末のセキュリティレベルが所定レベルに達しないときにアクセス許可範囲をセキュリティ設定案内サーバ６、ウイルス情報サーバ５に変更することを示した。

【００５３】

しかしながら、本発明の実施形態はこれに限らず、アクセス許可範囲の初期設定をセキュリティ設定案内サーバ６、ウイルス情報サーバ５にしておき、端末のセキュリティレベルが所定レベルに達したときにアクセス許可範囲を全ての範囲に変更する実施形態としてもよい。すなわち、この実施形態を実現するには、セキュリティ管理装置１０を以下のように構成すればよい。

【００５４】

まず、セキュリティ管理装置１０のセキュリティ検出部１１が、端末２のセキュリティレベルを検出する方法は先の実施形態と同様である。

【００５５】

判定部１２は、端末２からのアクセスがあった場合、端末２のセキュリティレベルが所定のセキュリティレベルに達しているか否かを判定する。この判定方法も先の実施形態と同様である。

【００５６】

そして、端末２のセキュリティレベルが所定のセキュリティレベルに達していると判定部１２で判定した場合、すなわちアクセス許可対象と判定した場合、アクセス制御部３はアクセス許可範囲を初期設定とされているセキュリティ設定案内サーバ６、ウイルス情報サーバ５から全ての範囲（全てのコンピュータ）に変更して、その端末２がどのコンピュータに対してもアクセスできるようにルーティングを行う。

【００５７】

一方、前記端末２のセキュリティレベルが所定のセキュリティレベルに達していないと判定部１２で判定した場合、すなわちアクセス許可対象でないと判定した場合、アクセス制御部３はアクセス許可範囲を初期設定とされているセキュリティ設定案内サーバ６、ウイルス情報サーバ５のままとする。その後のアクセス制御部３による端末２のセキュリティレベルを変更させる処理については先の実施形態と同様である。

【００５８】

また、上記実施形態では、セキュリティ検出部１１によるセキュリティレベルの検出方法として、前記端末２がサーバ５に所定間隔でアクセスしたか否か（アクセスパターン）で検出したが、これに限らず、セキュリティ管理装置１が端末２によるアクセス履歴を記録しておき、そのアクセス履歴を用いて端末２のセキュリティレベルを検出するようにしてもよい。

【００５９】

例えば、端末２が他のコンピュータへアクセスする場合に、セキュリティ管理装置１が端末２から送信されたデータパケットを受信し、そのデータパケットに

含まれる宛先アドレスと送信元のアドレス（端末２のアドレス）およびそのデータパケットを受信した日時情報をアクセス履歴として記録しておく。

【００６０】

そして、端末２から他のコンピュータへのアクセス要求があった場合に、アクセス履歴からその端末２がウイルス情報サーバ５にアクセスした最新の日時を求め、このアクセスした最新の日時が所定日時より前であればセキュリティレベルが低い、或はアクセスした最新の日時が所定日時より後であればセキュリティレベルが高いなどのようにセキュリティレベルを検出してもよい。

【００６１】

また、以下に付記した構成であっても前述の実施形態と同様の効果を得ることができる。

【００６２】

（付記１）

端末のセキュリティレベルを検出するセキュリティ検出部と、

前記端末のセキュリティレベルと所定のレベルとを比較判定する判定部と、

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、当該端末のアクセス許可範囲を制限するアクセス制御部と、

を備えたセキュリティ管理装置。

【００６３】

（付記２）

前記アクセス制御部は、前記端末のセキュリティレベルが所定のレベルに達していると前記判定部で判定された場合、前記制限範囲より広範囲を当該端末のアクセス許可範囲とする付記１に記載のセキュリティ管理装置。

【００６４】

（付記３）

前記アクセス制御部は、前記端末の通信経路を選択する機能を備え、前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合に、当該端末の通信先を特定の装置に変更する付記１に記載のセキュリティ管理装置。

【００６５】

（付記４）

前記特定の装置が前記端末のセキュリティレベルを設定する、或は設定の案内を当該端末に提供する付記３に記載のセキュリティ管理装置。

【００６６】

（付記５）

コンピュータが、

端末のセキュリティレベルを検出するステップと、

前記端末のセキュリティレベルと所定のレベルとを比較判定するステップと、

前記端末のセキュリティレベルが所定のレベルに達していないと判定された場合、当該端末のアクセス許可範囲を制限するステップと、

を実行するセキュリティ管理方法。

【００６７】

（付記６）

前記端末のセキュリティレベルが所定のレベルに達していると判定された場合、前記制限範囲より広範囲を当該端末のアクセス許可範囲とするステップを含む付記５に記載のセキュリティ管理方法。

【００６８】

（付記７）

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、前記端末のアクセス許可範囲を制限するステップにおいて、

当該端末の通信経路を選択して通信先を特定の装置に変更する付記５に記載のセキュリティ管理方法。

【００６９】

（付記８）

前記特定の装置が前記端末のセキュリティレベルを設定する、或は設定の案内を当該端末に提供する付記７に記載のセキュリティ管理方法。

【００７０】

（付記９）

端末のセキュリティレベルを検出するステップと、

前記端末のセキュリティレベルと所定のレベルとを比較判定するステップと、

前記端末のセキュリティレベルが所定のレベルに達していないと判定された場合、当該端末のアクセス許可範囲を制限するステップと、

をコンピュータにより実行可能なセキュリティ管理プログラム。

【００７１】

（付記１０）

前記端末のセキュリティレベルが所定のレベルに達していると判定された場合、前記制限範囲より広範囲を当該端末のアクセス許可範囲とするステップを含む付記９に記載のセキュリティ管理プログラム。

【００７２】

（付記１１）

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、前記端末のアクセス許可範囲を制限するステップにおいて、

当該端末の通信経路を選択して通信先を特定の装置に変更する付記９に記載のセキュリティ管理プログラム。

【００７３】

（付記１２）

前記特定の装置が前記端末のセキュリティレベルを設定する、或は設定の案内を当該端末に提供する付記１１に記載のセキュリティ管理プログラム。

【００７４】

（付記１３）

セキュリティ管理装置と、ユーザ用の端末と、セキュリティ設定案内装置とをネットワークを介して接続したセキュリティ管理システムとして構成し、

端末のセキュリティレベルを検出するセキュリティレベル検出部と、

前記端末のセキュリティレベルと所定のレベルとを比較判定する判定部と、

前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合、当該端末のアクセス許可範囲を制限するアクセス制御部と、

を備えたことを特徴とするセキュリティ管理システム。

【００７５】

（付記１４）

前記アクセス制御部は、前記端末のセキュリティレベルが所定のレベルに達していないと前記判定部で判定された場合に、当該端末を前記セキュリティ設定案内装置に接続させる付記１３に記載のセキュリティ管理システム。

【００７６】

本発明において、以上の構成要素は可能な限り組み合わせることができる。

【００７７】

【発明の効果】

以上説明したように、本発明によれば、セキュリティ管理装置が端末のセキュリティレベルに応じて該端末のアクセス制御を行い、セキュリティ設定を促すことにより、セキュリティ管理の省力化を図りつつ所望のセキュリティを確保する技術を提供することができる。

【図面の簡単な説明】

【図１】　セキュリティ管理装置を備えたネットワーク構成例を示す図

【図２】　セキュリティ管理装置の構成を示すブロック図

【図３】　セキュリティ管理手順を示す説明図

【図４】　設定を案内する画面の表示例

【図５】　変形例１のセキュリティ管理装置の構成を示すブロック図

【図６】　実施形態２のセキュリティ管理装置の構成を示すブロック図

【図７】　実施形態２のネットワークの構成図

【符号の説明】

1　　セキュリティ管理装置

2　　端末

2　　該端末

3　　ファイアウォール

4　　インターネット

５　　ウイルス情報サーバ

６　　セキュリティ設定案内サーバ

１０　セキュリティ管理装置

１１　セキュリティ検出部

１２　判定部

１３　アクセス制御部

１４　メール受信部

１５　メール送信部

２０　メールサーバ

２１　本体

２２　演算処理部

２３　記憶装置

２４　入出力部

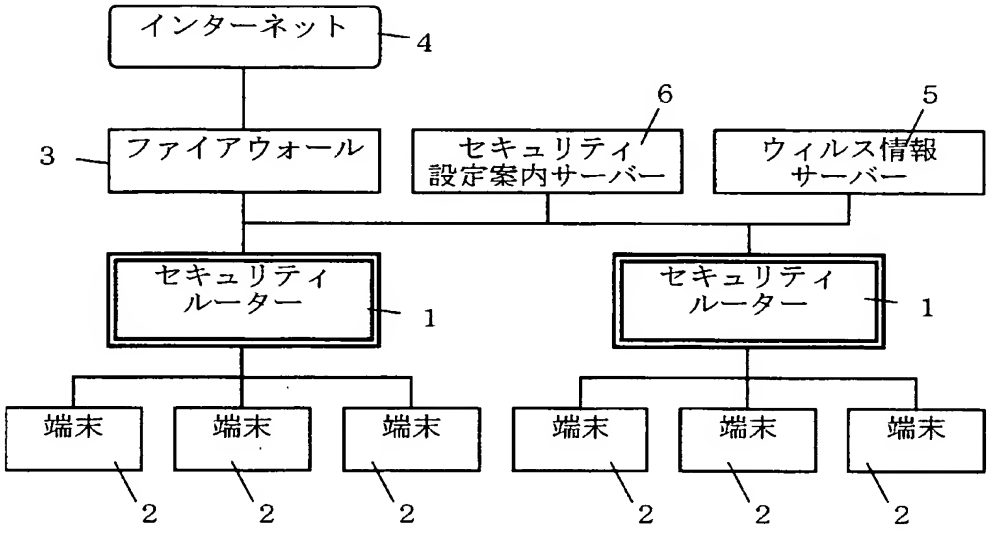
２５　ＣＣＵ（通信制御装置）

９９　ボタン

【書類名】　図面

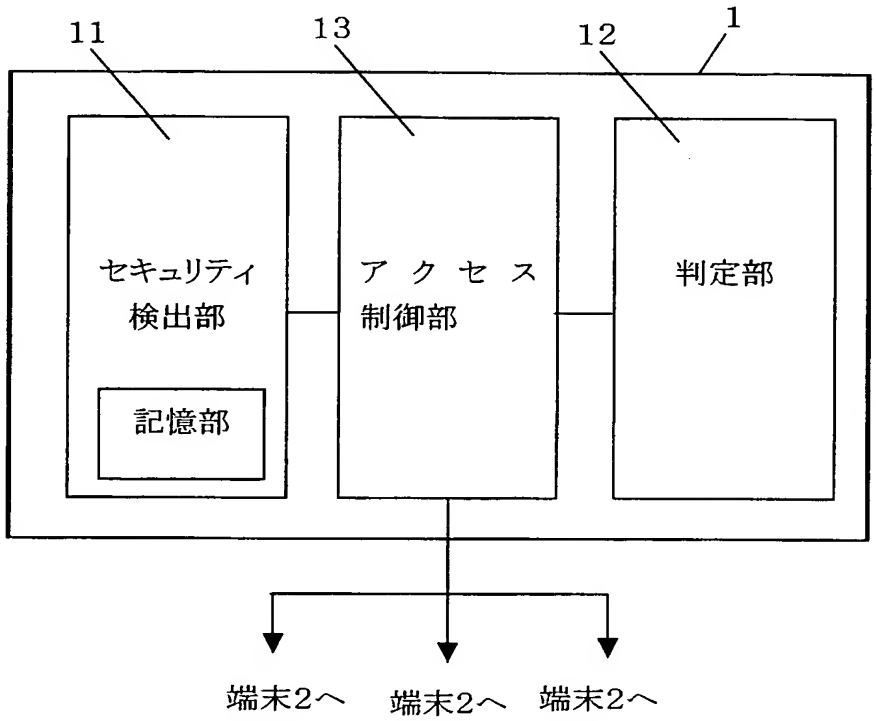
【図１】

セキュリティ管理装置を備えたネットワーク構成例を示す図

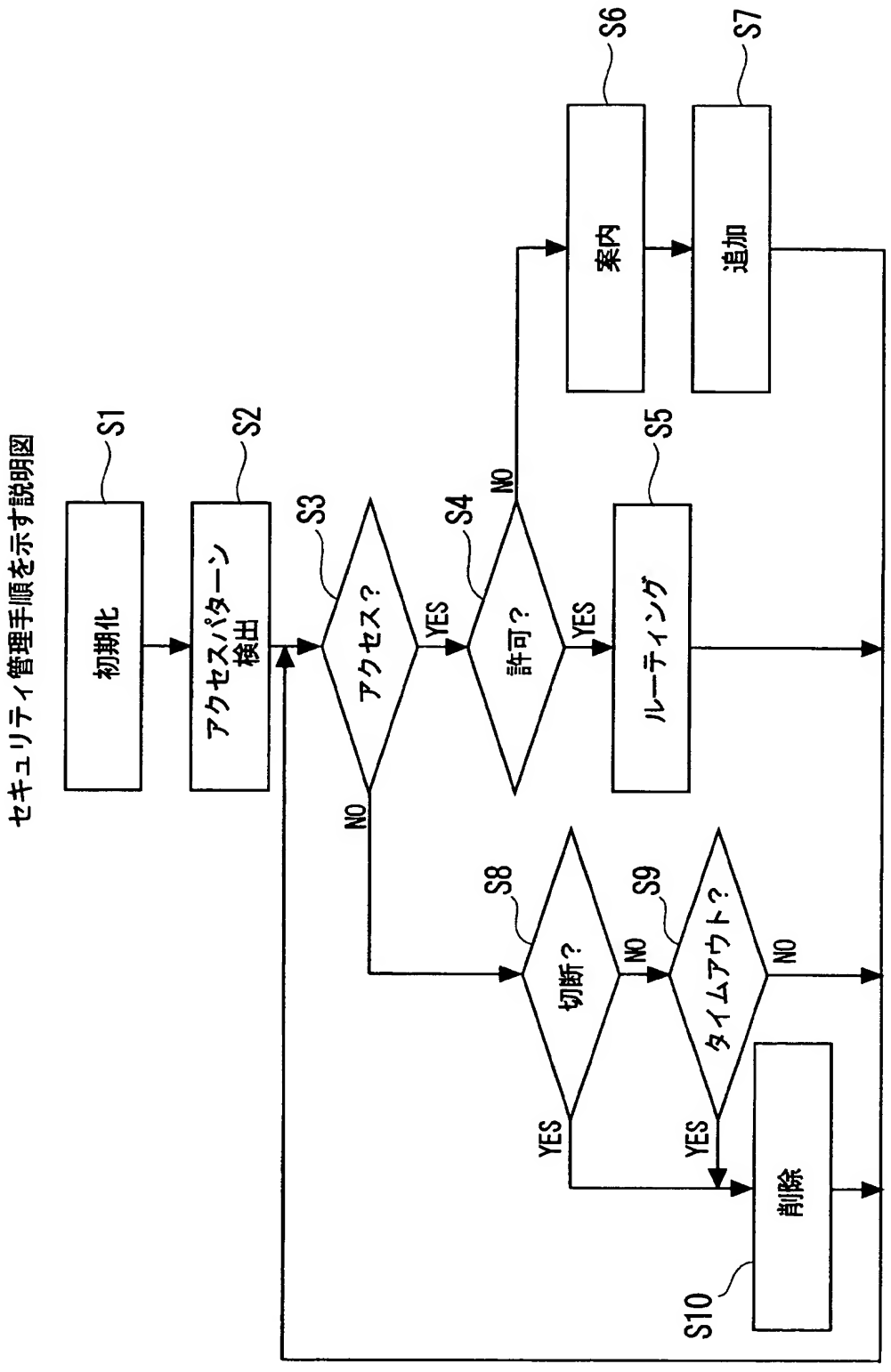


【図２】

セキュリティ管理装置の構成を示すブロック図

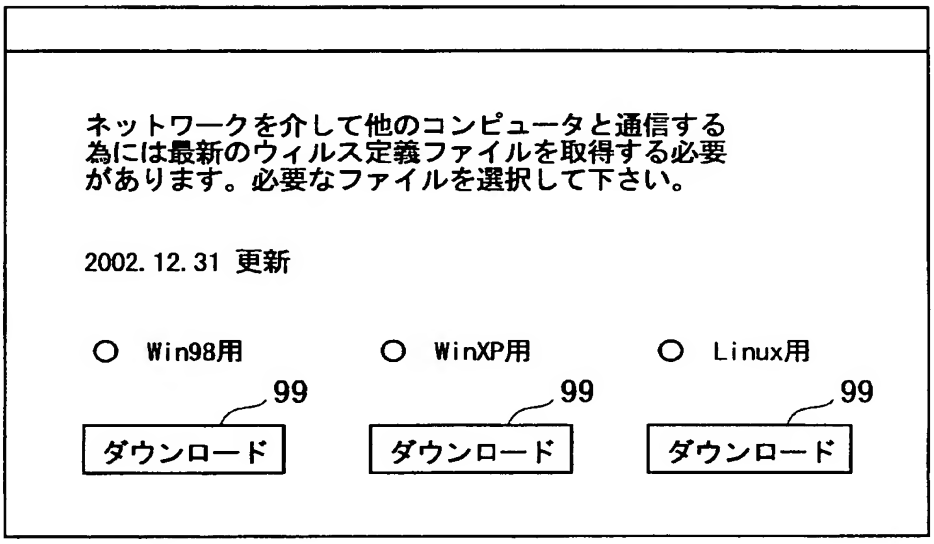


【図３】


セキュリティ管理手順を示す説明図
S1
初期化
S2
アクセスパターン検出
S3
アクセス？
YES
S4
許可？
NO
YES
S5
ルーティング
S6
案内
S7
追加
NO
S8
切断？
NO
S9
タイムアウト？
NO
YES
YES
削除
S10

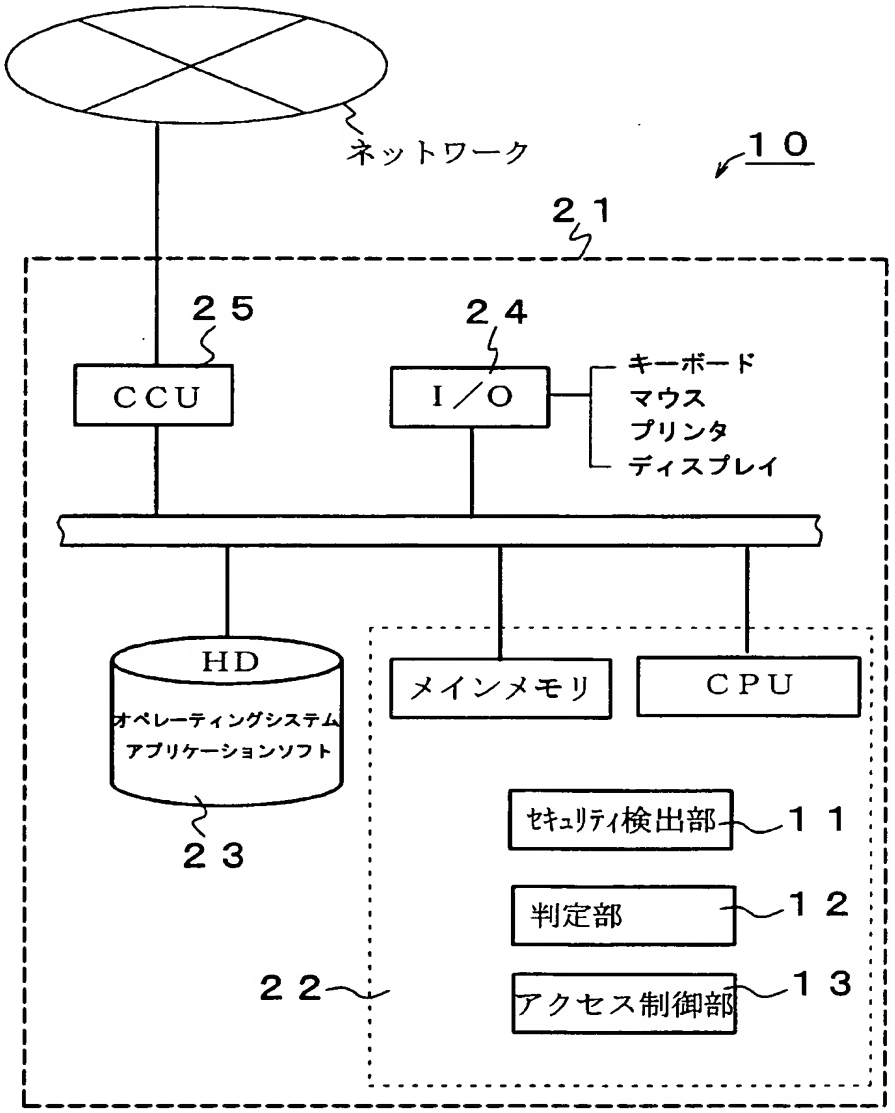
【図４】

設定を案内する画面の表示例



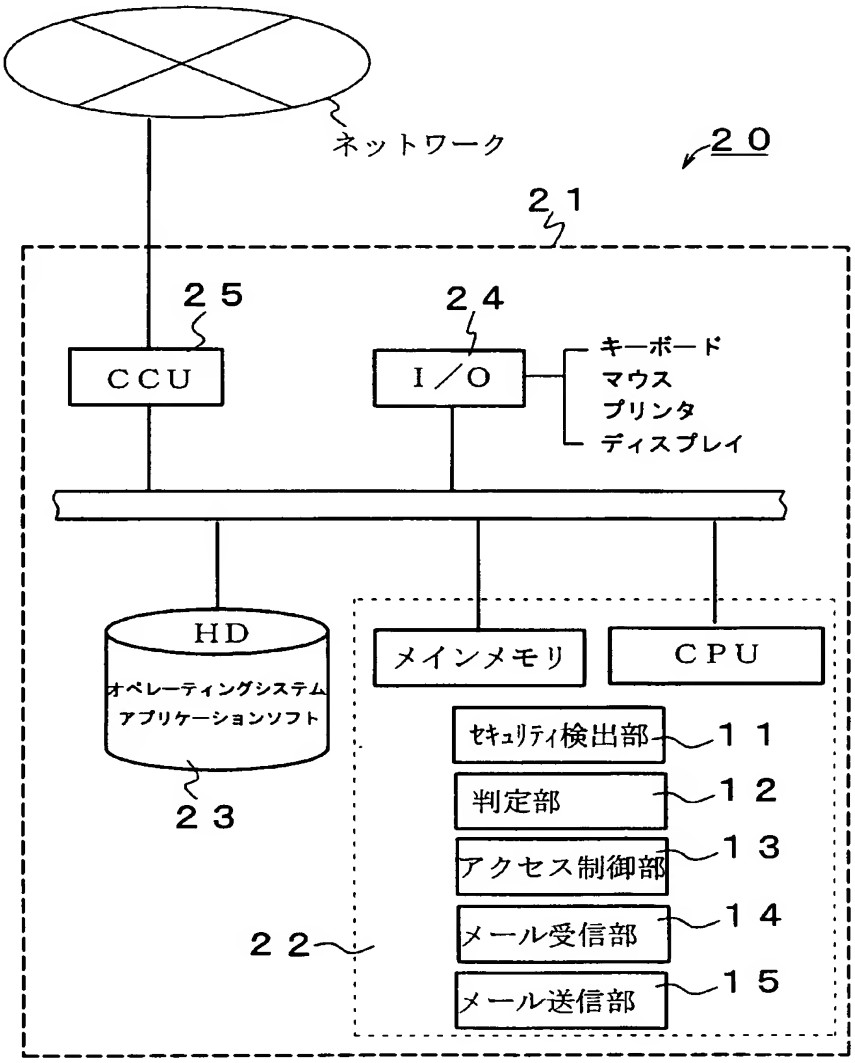
【図５】

変形例１のセキュリティ管理装置の構成を示すブロック図



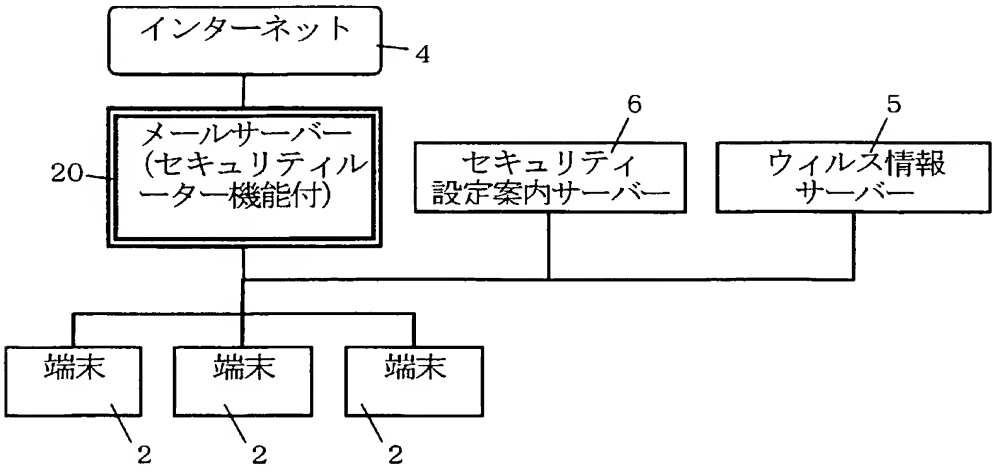
【図６】

実施形態２のセキュリティ管理装置の構成を示すブロック図



【図７】

実施形態２のネットワークの構成図



【書類名】　　要約書

【要約】

【課題】　セキュリティ管理装置が端末のセキュリティレベルに応じて該端末のアクセス制御を行い、セキュリティ設定を促すことにより、セキュリティ管理の省力化を図りつつ所望のセキュリティを確保可能なセキュリティ管理装置、セキュリティ管理方法、セキュリティ管理プログラム、セキュリティ管理システムを提供する。

【解決手段】　アクセスパターンによって端末のセキュリティレベルを検出して、前記セキュリティレベルが所定のレベルに達しているか否かを判定し、前記端末のセキュリティレベルが所定のレベルに達していないと判定された場合に、当該端末のアクセス許可範囲を変更する。

【選択図】　　図１

特願２００３－０２２６３０

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社